**Table of Contents**

[Cybersecurity Incident Playbook and Plan 1](#_Toc198344196)

[Insurance Coordination and Vendor Pre-Approval 1](#_Toc198344197)

[Preventive Security Measures 2](#_Toc198344198)

[Initial Response Directions 3](#_Toc198344199)

[Do's and Don'ts During an Incident 5](#_Toc198344200)

[Phases of Response 6](#_Toc198344201)

[Roles and Responsibilities Overview 8](#_Toc198344202)

[Roles and Responsibilities Directory 9](#_Toc198344203)

[Business Impact Analysis 10](#_Toc198344204)

[Backup and Recovery Strategy 11](#_Toc198344205)

[Communication Guidelines 13](#_Toc198344206)

[Ransom Payment Considerations 13](#_Toc198344207)

[Incident Lifecycle Timeline (Industry Averages) 14](#_Toc198344208)

[Severity Classification Matrix 15](#_Toc198344209)

[Incident Logging and Tracking Template 15](#_Toc198344210)

[Regulatory and Compliance Mapping 15](#_Toc198344211)

[Third-Party Vendor Notification Process 16](#_Toc198344212)

[Evidence Handling & Chain of Custody Procedures 16](#_Toc198344213)

[System Reintegration Protocol 17](#_Toc198344214)

[Tabletop Exercise Template 17](#_Toc198344215)

[Financial Impact Assessment Worksheet 17](#_Toc198344216)

[Disclaimer 18](#_Toc198344217)

# Cybersecurity Incident Playbook and Plan

**Storage Note**: This document should never be stored on any company network, shared drive, or endpoint device. If accessed during a cybersecurity incident, it could provide adversaries with valuable insight into your defenses, procedures, and contact protocols. Instead, keep printed copies securely stored onsite and offsite in labeled binders accessible to authorized personnel only. As an additional secure option, the document may be stored on a *removable, physically disconnected storage device* (e.g., encrypted USB drive) kept in a secure location and only connected when updates are needed.

*In the face of a cybersecurity incident, uncertainty is the enemy—clarity is the defense.* This Cybersecurity Incident Playbook is a mission-critical guide designed to help **[COMPANY]** respond with precision, speed, and confidence. It outlines a clear, step-by-step process for detecting, analyzing, containing, eradicating, and recovering from security incidents. More than just a document, it is a frontline tool that equips our team with predefined roles, communication protocols, escalation paths, and recovery strategies assuring that when systems are disrupted, the response is swift, coordinated, and effective. This plan is built not just to navigate cybersecurity incidents, but to emerge stronger from them.

# Insurance Coordination and Vendor Pre-Approval

To ensure a smooth response and uninterrupted claims process, **[COMPANY]** should proactively schedule a meeting with its cyber insurance carrier and assigned agent to:

* Review the entire Incident Response Plan
* Obtain formal buy-in for the procedures outlined
* Secure pre-approval for any preferred IR forensic response vendors

This meeting ensures all parties are aligned on expectations, policy limits, notification timelines, and vendor eligibility **before** an incident occurs. Any requested changes from the insurer should be documented and approved by the Executive Sponsor and Legal and Compliance Liaison.

This step should be revisited annually or whenever the cyber insurance policy is updated or renewed.

# Preventive Security Measures

Preventing incidents before they occur is a cornerstone of any strong cybersecurity posture. This section outlines baseline security best practices that should be implemented and maintained to significantly reduce risk across the organization.

## Access Controls & Identity Management

* **Multi-Factor Authentication (MFA)**: Enforce MFA on all user accounts, especially administrative and remote access.
* **Least Privilege Access**: Ensure users have only the access needed for their job functions.
* **Password Policy**: Enforce strong password requirements and regular updates.

## Recommended Backup Strategy

To prepare for system recovery and business continuity, implement a multi-layered and fully automated backup solution:

* **Image-Based Backups**: Automatically capture full system snapshots several times daily.
* **Local Backups**: Store automated backups on secured local appliances for rapid restore.
* **Offsite Replication**: Replicate backups to an offsite location or secondary office.
* **Immutable Storage**: Use immutable storage to protect backups from alteration or deletion by ransomware.
* **Virtualization**: Maintain capability for virtualization of systems both onsite and in the cloud to support rapid recovery.
* **Automated Backup Testing**: Schedule regular, automated testing of backup integrity and restorability.
* **Daily Monitoring**: Ensure both backups and backup testing results are reviewed and verified daily by designated personnel.

## Additional Preventive Measures

* **Cyber Insurance Policy Storage**: Never store your cyber insurance policy on the network. Threat actors often seek out these documents to learn the details of your coverage, including policy limits, which they may then use to shape their ransom demands. In the event of a ransomware or system-wide incident, access to digital documents may be disrupted or denied. Maintain printed copies of the policy in a clearly labeled binder, stored both **onsite** and at a secure **offsite** location. This ensures rapid access to critical policy terms, contact numbers, and response procedures even when digital systems are unavailable, and keeps sensitive insurance information out of reach from attackers.
* **Zero Trust Architecture**: Adopt a Zero Trust model that assumes no user or device is trustworthy by default, enforcing strict verification at every application access point.
* **EDR/MDR (Endpoint & Managed Detection and Response)**: Utilize advanced endpoint protection and consider managed services for 24/7 monitoring and response capabilities.
* **Next-Generation Antivirus (NGAV)**: Deploy NGAV tools that use behavioral analysis, AI, and machine learning to detect and block sophisticated threats before they cause harm.
* **Patch Management**: Regularly update and patch systems and applications.
* **Endpoint Detection and Response (EDR)**: Deploy advanced security tools with behavioral analytics.
* **Security Awareness Training**: Conduct recurring staff training on phishing, social engineering, and policy adherence.
* **Email Filtering & Threat Protection**: Implement tools to detect and block suspicious emails and attachments.
* **Vulnerability Scanning**: Run internal and external scans regularly to identify potential weak points.

***Note****:* These preventive measures should be reviewed quarterly and updated based on evolving threat landscapes and regulatory changes.

# Initial Response Directions

When a cybersecurity incident is suspected or confirmed, taking the right immediate steps is critical to preserve data, prevent further damage, and support investigation and recovery efforts. The following steps should be executed as soon as the incident is detected:

## Step-by-Step Initial Response Actions

### Disconnect Internet Connectivity

* + Immediately disconnect all affected systems or networks from the internet.
	+ Disable Wi-Fi, unplug network cables, or shut off switch/router uplinks as appropriate.
	+ Do **not** power off systems—leave all machines powered on to preserve volatile memory (RAM) for forensic investigation.

### Preserve the Scene

* + Avoid interacting with affected systems beyond what is necessary to disconnect them.
	+ Do not attempt to delete files, run antivirus scans, or “clean” the system.
	+ Record any visible alerts or symptoms and take screenshots if possible.

### Notify the Incident Response Coordinator

* + Contact the designated Incident Response Coordinator immediately.
	+ Provide a concise summary of the observations and steps already taken.

### Document Everything

* + Begin a log of actions taken, including dates, times, who was involved, and what was observed.
	+ Include any emails, messages, alerts, or anomalies that led to detection.

### Notify Legal and Insurance

* + Contact the Legal and Compliance Liaison to initiate any regulatory or contractual notifications.
	+ Notify the designated Insurance Agent or 24/7 contact as outlined in the Roles and Responsibilities Directory.

### Activate the Incident Response Plan

* + The Incident Response Coordinator will assess the situation and initiate the appropriate phase from the full incident response plan.

***Note****:* These directions should be printed and readily accessible at all critical workstations, network closets, and by all key personnel.

# Do's and Don'ts During an Incident

While fast action is critical, certain steps must be taken—and others avoid supporting investigation and recovery. Below are the best practices for each:

## DOs

* **Do document everything** — Maintain a detailed timeline of actions, observations, and communications.
* **Do notify the right people immediately** — Escalate quickly to the Incident Response Coordinator and legal/insurance contacts.
* **Do use secure communication channels** — Use approved methods like secure messaging or direct phone calls. **Never use email** to communicate about an ongoing incident, especially if the email system is suspected of being compromised. — Use approved methods like secure messaging or direct phone calls.
* **Do isolate the problem** — Disconnect affected systems from the network without powering them off.
* **Do preserve the environment** — Maintain the current system state for forensic analysis.
* **Do remain calm and follow procedure** — Stick to the plan and use this playbook as your guide.

## DON’Ts

* **Do NOT power off affected machines** — This can destroy critical evidence held in volatile memory (RAM).
* **Do NOT delete, move, or alter files** — This includes suspicious files or any potentially affected documents.
* **Do NOT run antivirus or anti-malware scans** — These can quarantine or remove files needed for forensic analysis.
* **Do NOT attempt to “clean” or restore systems before guidance** — Restoration before analysis can eliminate valuable clues.
* **Do NOT communicate about the incident through email or compromised systems** — Use designated secure channels only.
* **Do NOT discuss the incident with clients, vendors, or press** — Refer all inquiries to the Communications Officer.
* **Do NOT delay notification to the Incident Response Coordinator** — Time is critical.
* **Do NOT rely on memory** — All actions and observations must be documented in real-time.

Following these precautions helps preserve forensic integrity, reduce liability, and streamline recovery.

# Phases of Response

A structured response is essential to minimizing the impact of a cybersecurity incident and restoring normal operations. **[COMPANY]**’s incident response process is divided into six distinct phases, each serving a critical purpose in the overall strategy:

## 1. Preparation

Preparation is the foundation of incident response. This phase ensures that **[COMPANY]** has the tools, policies, and trained personnel needed to effectively manage security incidents. It includes:

* Documented incident response procedures
* Regular training and simulation exercises
* Defined roles and responsibilities
* Maintained contact lists and communication protocols
* Up-to-date asset and data inventory

## 2. Identification

During this phase, the goal is to determine whether an event qualifies as a security incident. Key activities include:

* Monitoring systems for anomalous behavior
* Validating alerts from detection tools
* Documenting signs of incident
* Notifying stakeholders as necessary

## 3. Containment

Once an incident is confirmed, containment efforts aim to limit its scope and prevent further damage. This may involve:

* Isolating affected systems
* Applying temporary fixes
* Preserving forensic evidence
* Activating communication protocols

## 4. Eradication

With containment in place, the next step is to remove the root cause of the incident from the environment. This may include:

* Removing malware or unauthorized access points
* Applying patches or updates
* Hardening system configurations

## 5. Recovery

This phase focuses on restoring systems and operations to normal while ensuring that vulnerabilities have been addressed. Key actions:

* Restoring from well-known backups
* Monitoring systems for signs of re-infection or incidents
* Validating system integrity and performance

## 6. Lessons Learned

After the incident is resolved, **[COMPANY]** conducts a thorough review to identify strengths, weaknesses, and opportunities for improvement. This includes:

* A formal post-incident report
* Root cause analysis
* Updates to the incident response plan
* Additional training or policy changes as needed

# Roles and Responsibilities Overview

To ensure a fully aligned and compliant response effort, **[COMPANY]** must proactively coordinate with its cyber insurance stakeholders.

## Pre-Incident Coordination

* A meeting should be held with both the **Insurance Carrier** and **Insurance Agent** to review this Incident Response Plan in full.
* The goal is to gain their **buy-in**, verify that all recovery and investigation procedures are within the scope of the policy, and secure **pre-approval for any preferred forensic vendors** or IR response teams.
* All feedback or required changes to align with the insurance contract should be reviewed, approved, and documented by the Legal and Compliance Liaison and the Executive Sponsor.

This coordination should be revisited annually or anytime the cyber insurance policy changes.

A clearly defined chain of command and division of duties ensures a coordinated and efficient response to any cybersecurity incident. Below is an outline of the primary roles involved in **[COMPANY]**’s incident response efforts:

## Incident Response Coordinator

* Oversees the entire incident response process
* Acts as the primary decision-maker during an incident
* Coordinates cross-functional teams and ensures timely communication

## IT Security Lead

* Leads the technical analysis of the incident
* Coordinates containment, eradication, and recovery efforts
* Maintains forensic integrity of affected systems

## Communications Officer

* Manages internal and external communications
* Ensures consistent messaging to staff, partners, and—if applicable—clients
* Coordinates with legal and compliance teams

## Legal and Compliance Liaison

* Evaluates potential regulatory impacts
* Provides legal counsel and documentation guidance
* Coordinates with law enforcement or third-party investigators when necessary

## Executive Sponsor / Leadership

* Approves high-level decisions and resource allocation
* Maintains strategic oversight and business continuity alignment

# Roles and Responsibilities Directory

In the event of a cybersecurity incident, **[COMPANY]** may be subject to mandatory reporting requirements imposed by regulatory authorities, contractual agreements, or government contracts. It is critical to identify and act upon these obligations swiftly to ensure compliance and avoid legal or financial penalties.

## Key considerations include:

* **Government Contracts**: Many federal, state, or local contracts include clauses that require immediate or time-bound incident reporting to specified government agencies or contract officers.
* **Industry-Specific Regulations**: Depending on the sector, organizations may be subject to specific cybersecurity incident reporting mandates such as those under HIPAA, GLBA, DFARS, CMMC, or others.
* **Client and Vendor Agreements**: Contractual obligations may require notification of clients, vendors, or third-party stakeholders within a defined timeframe.
* **Insurance Notification Windows**: Timely notification to the cyber insurance provider is often a requirement of coverage.

All reporting obligations must be clearly documented, with contacts, deadlines, and procedures outlined and maintained in the Compliance Register. The Legal and Compliance Liaison is responsible for ensuring all relevant notifications are completed appropriately.

Action Required: Review all existing contracts and regulatory commitments and update this plan with a list of required notifications, associated timelines, and responsible parties.

## Mandated Notification Requirements Form

Use the following table to track and maintain generic notification requirements. This form should be reviewed and updated regularly by the Legal and Compliance Liaison:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Notification Label** | **Description of Obligation** | **Timeframe** | **Contact / Agency** | **Contact Info** | **Notes** |
| Notification 1 | [Insert description] | [Insert time] | [Insert contact or agency] | [Insert contact info] | *[Insert notes]* |
| Notification 2 | [Insert description] | [Insert time] | [Insert contact or agency] | [Insert contact info] | *[Insert notes]* |
| Notification 3 | [Insert description] | [Insert time] | [Insert contact or agency] | [Insert contact info] | *[Insert notes]* |
| Notification 1 | [Insert description] | [Insert time] | [Insert contact or agency] | [Insert contact info] | *[Insert notes]* |
| Notification 5 | [Insert description] | [Insert time] | [Insert contact or agency] | [Insert contact info] | *[Insert notes]* |

# Business Impact Analysis

A Business Impact Analysis (BIA) identifies critical business assets and evaluates the consequences of a disruption. The objective is to prioritize recovery efforts to ensure that **[COMPANY]** can resume essential operations in an efficient and structured manner.

## Instructions:

1. Identify and list critical assets below.
2. Prioritize recovery based on business impact, such as legal obligations, financial continuity, or operational criticality. For example, if union payroll must be submitted by Wednesday to avoid significant fines, the accounting system should be prioritized accordingly.
3. Assign each a recovery priority from 1 (highest) to 10 (lowest).
4. Briefly describe the asset's purpose and impact on the business.

This section is to be updated periodically and reviewed during disaster recovery testing.

### Top 10 Priority Assets for Recovery

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Priority** | **Asset Name** | **Description** | **Owner/Department** | **Notes** |
| 1 | Domain Controller | Primary security, authentication, and account directory for the network. | [Insert Owner] | *[Insert notes]* |
| 2 | Accounting System | Financial operations including payroll, invoicing, and compliance. | [Insert Owner] | *[Insert notes]* |
| 3 | Email Server | Central communication platform for internal and external messages. Ahmad  | [Insert Owner] | *[Insert notes]* |
| 4 | File Server | Houses shared documents critical to daily operations. | [Insert Owner] | *[Insert notes]* |
| 5 | Line-of-Business App | Core application for daily operational activities. | [Insert Owner] | *[Insert notes]* |
| 6 | Backup Management | Ensures access to current and historical backups for all major systems. | [Insert Owner] | *[Insert notes]* |
| 7 | CRM System | Customer records and engagement data vital to client relationships. | [Insert Owner] | *[Insert notes]* |
| 8 | Remote Access Gateway | Facilitates secure off-site connectivity for staff and contractors. | [Insert Owner] | *[Insert notes]* |
| 9 | Inventory Database | Tracks product/material stock levels and supply chain dependencies. | [Insert Owner] | *[Insert notes]* |
| 10 | VOIP Phone System | Telephone communications for client support and operations. | [Insert Owner] | *[Insert notes]* |

***Note***: Customize this list based on the actual operational structure and systems of **[COMPANY]**.

# Backup and Recovery Strategy

A well-documented and validated backup strategy is critical to ensuring that **[COMPANY]** can recover essential data and systems in the aftermath of a cybersecurity incident. This section outlines the core backup infrastructure, recovery methods, testing schedule, and contact responsibilities.

## Backup Solution Overview

* **Backup Type**: [e.g., Image-based, File-level, Incremental, Full]
* **Backup Frequency**: [e.g., Hourly, Daily, Weekly]
* **Retention Policy**: [e.g., 30 days, 6 months, 1 year]
* **Storage Locations**: [e.g., On-site appliance, Offsite vault, Cloud backup]
* **Encryption Method**: [e.g., AES-256 encryption in transit and at rest]
* **Monitoring & Alerts**: [e.g., Automated alerts for backup success/failure]

## Recovery Methods

* **File-Level Recovery**: Used for restoration of individual files or directories.
* **Bare-Metal Restore**: Full system recovery to the same or different hardware.
* **Virtual Machine Failover**: Instant recovery by spinning up systems in a virtualized environment.
* **Cloud-Based Recovery**: Access to cloud-hosted recovery environments in case of on-premise failure.

## Responsibilities

* **Backup Administrator**: [Insert Name & Contact] — Monitors backup health and integrity.
* **Recovery Lead**: [Insert Name & Contact] — Executes recovery processes as needed.
* **Testing Coordinator**: [Insert Name & Contact] — Schedules and documents recovery drills.

## Backup Testing Schedule

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Test Type** | **Frequency** | **Last Tested** | **Result Summary** | **Next Scheduled Test** |
| File Recovery | [e.g., Monthly] | [Insert Date] | [Insert Notes] | [Insert Date] |
| Full System Restore | [e.g., Quarterly] | [Insert Date] | [Insert Notes] | [Insert Date] |
| Cloud Failover Test | [e.g., Annually] | [Insert Date] | [Insert Notes] | [Insert Date] |

***Note****:* This section must be reviewed and updated after each major change to the backup system or vendor.

# Communication Guidelines

During any cybersecurity incident, it is imperative that consistent and legally sound terminology is used. All internal staff, contractors, and vendors must refer to such events solely as **"incidents"**. The use of terms such as "breach" or "compromise" is strictly prohibited unless explicitly authorized by legal counsel or the executive team.

Only the **Communications Officer** is authorized to speak with the media, external stakeholders, or regulatory bodies. This includes both official and unofficial statements or comments regarding the incident. No other employee, contractor, or vendor shall provide public commentary or formal notification without written approval from the executive leadership.

If clients or vendors inquire about the situation, all personnel should respond with a consistent, approved statement such as:

"We're currently looking into an incident, and as soon as there's an update, we'll make sure you're informed. We appreciate your patience and understanding."

This policy ensures unified messaging, minimizes legal risk, and supports compliance with all contractual and regulatory requirements.

[Insert description] | [Insert time] | [Insert contact or agency] | [Insert contact info] | [Insert notes]

# Ransom Payment Considerations

In the event of a ransomware incident, **[COMPANY]** must carefully evaluate whether to engage with threat actors or consider ransom payment. While paying a ransom may appear to offer a quick path to recovery, it introduces legal, ethical, and operational risks.

## Key Considerations:

* **Legal Restrictions**: Some jurisdictions prohibit or heavily regulate ransom payments. Payments to sanctioned entities can carry severe penalties.
* **Insurance Requirements**: The cyber insurance provider must be notified prior to any consideration of payment. They may have requirements or limitations that impact this decision.
* **Law Enforcement Notification**: Contacting law enforcement or cybercrime units is recommended and may be required by policy.
* **Data Recovery Alternatives**: Confirm that all recovery options have been explored, including restoring from backups.
* **Intellectual Property Exposure**: Evaluate the risk of critical business information, trade secrets, or proprietary systems being sold or leaked. Threat actors may threaten to release or monetize intellectual property (IP) publicly to create pressure. Consider the potential long-term damage to competitive advantage, regulatory obligations, and trust.
* **Third-Party Harassment**: Be aware that threat actors have been known to extract client and vendor contact lists and pressure external stakeholders by threatening them or publicly releasing stolen data to force a ransom payment. This tactic can escalate reputational damage and add additional external pressure to respond.
* **Reputation and Precedent**: Paying a ransom can encourage future targeting and may harm your organization’s reputation.
* **Likelihood of Data Return**: There is no guarantee that payment will result in data decryption or deletion.

The final decision should involve executive leadership, legal counsel, the insurance carrier, and law enforcement, with clear documentation of the rationale and risk analysis.

# Incident Lifecycle Timeline (Industry Averages)

Understanding the average timeline of a cybersecurity incident can help set realistic expectations and guide planning. The following are typical phases and durations observed across industries:

|  |  |  |
| --- | --- | --- |
| **Phase** | **Day Range** | **Description** |
| **Day 0 – Initial Compromise** | Day 0 | The attacker gains unauthorized access, often undetected. |
| **Discovery & Detection** | Day 5–Day 21 | On average, it takes 5–21 days for a business to detect suspicious activity. |
| **Containment Initiated** | Day 21–Day 30 | Incident Response begins containment of affected systems. |
| **Investigation & Forensics** | Day 30–Day 60 | Forensic experts analyze the scope, impact, and origin of the incident. |
| **Communication & Reporting** | Day 30–Day 60+ | Notifications are issued to insurers, clients, regulators (if required). |
| **System Recovery** | Day 45–Day 90 | Systems are restored from backups, vulnerabilities patched, and normal operations resume. |
| **Post-Incident Review** | Day 90–Day 120 | Internal debriefing, plan revisions, and corrective actions are implemented. |

***Note****:* Timelines vary based on preparedness, tools, staff availability, and attacker sophistication. Organizations with mature incident response programs may accelerate this timeline significantly.

# Severity Classification Matrix

Establishing clear severity levels ensures appropriate prioritization and response for each incident type. The following matrix outlines standard classification tiers:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Severity Level** | **Impact Scope** | **Urgency** | **Response Time** | **Example Incidents** |
| Critical | Enterprise-wide / public-facing impact | Immediate | Within 1 hour | Ransomware affecting core business systems |
| High | Multiple departments affected | High | Within 4 hours | Targeted phishing, active malware propagation |
| Medium | Single department or system affected | Moderate | Within 24 hours | Localized compromise, policy violations |
| Low | No direct impact / detected early | Routine | Within 3 days | Suspicious login, failed scans |

***Note****:* All incidents must be documented and escalated according to these classifications.

# Incident Logging and Tracking Template

Maintaining detailed logs during an incident is critical for accountability, forensics, and post-incident review. The table below should be used throughout the lifecycle of an incident:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Incident ID** | **Date/Time Detected** | **Detected By** | **Description** | **Affected Systems** | **Actions Taken** | **Current Status** | **Final Resolution** | **Notes** |
| [Insert ID] | [Insert Date/Time] | [Insert Name] | [Short summary] | [System(s)] | [Initial actions] | [Ongoing/Resolved] | [Resolution summary] | [Other notes] |

# Regulatory and Compliance Mapping

Certain regulations and contracts require formal incident reporting. This section maps key frameworks to incident response obligations:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Framework / Regulation** | **Notification Trigger** | **Reporting Deadline** | **Contact Required** | **Documentation Retention** |
| HIPAA | ePHI access/exposure | 60 days | OCR | 6 years |
| DFARS/CMMC | Controlled unclassified info (CUI) breach | 72 hours | DoD / DIBNet | 3 years |
| GDPR | Personal data breach | 72 hours | Supervisory Authority | Case-by-case |
| State Breach Laws | Personal Info (PII) | Varies by state | AG / Affected Individuals | Varies |

***Note****:* Legal and Compliance Liaison must verify requirements based on industry, location, and contract terms.

# Third-Party Vendor Notification Process

Vendors, partners, and third-party providers may be affected or need to be alerted during an incident. The process for managing such communication includes:

* Identify all vendors whose systems, services, or data may be impacted.
* Consult vendor contracts to verify notification requirements.
* Prepare pre-approved language from Communications Officer.
* Document notifications sent, time, recipient, and method.
* Track any vendor response actions or issues reported.

# Evidence Handling & Chain of Custody Procedures

Preserving and documenting digital evidence is essential for any investigation, especially when legal action or regulatory inquiry is possible. Guidelines include:

* Only authorized personnel (e.g., IR or Forensics Lead) may collect evidence.
* Record time/date, source system, and method of collection.
* Store evidence on write-protected, encrypted drives.
* Use a Chain of Custody form for each piece of evidence.
* Limit access and retain all logs for at least 3 years.

# System Reintegration Protocol

Before returning recovered systems into production, a formal validation process must occur:

1. Verify all malware or unauthorized access points are removed.
2. Reinstall clean software images from trusted sources.
3. Apply all critical patches and update configurations.
4. Run endpoint scans and validate system performance.
5. Have the Recovery Lead and Business Unit Owner sign off on reactivation.

# Tabletop Exercise Template

Simulated incident drills help assess readiness and refine procedures. Use the template below to plan and execute tabletop exercises:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Scenario Name** | **Objective** | **Departments Involved** | **Injects/Events** | **Success Criteria** | **Lessons Learned** |
| [Insert Name] | [Goal] | [List] | [Timeline of Events] | [Recovery time, decisions] | [Notes] |

Exercises should be held at least annually and whenever major system or policy changes occur.

# Financial Impact Assessment Worksheet

This worksheet can be used to estimate and record the direct and indirect costs of an incident:

|  |  |  |
| --- | --- | --- |
| **Cost Category** | **Estimated Value** | **Notes** |
| Downtime (hourly x hours) | [Insert] | [Insert Note] |
| Forensic Investigation | [Insert] | [Insert Note] |
| Legal/Compliance Fees | [Insert] | [Insert Note] |
| Communication/Public Relations | [Insert] | [Insert Note] |
| Insurance Deductible | [Insert] | [Insert Note] |
| Total Estimated Impact | [Sum] | [Insert Note] |

"Please ensure a current copy of the organization’s Cyber Insurance Policy is attached to this document, along with any other supporting materials."

# Disclaimer

This document is intended to serve as a general guide for establishing and managing a cybersecurity incident response process. It does **not** constitute legal advice or a formal representation of any insurance carrier. Users of this document should consult their own legal counsel and insurance representatives to ensure that all strategies, procedures, and terminology are aligned with applicable laws, regulations, and policy requirements.

**Attain Technology Inc.** assumes no liability for the use or implementation of this document without such independent review and professional guidance.